The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE (S) ISSUED:
12/14/2010

SUBJECT: Multiple Vulnerabilities in Internet Explorer Could Allow Remote Code Execution (MS10-090)

OVERVIEW:
Seven vulnerabilities have been discovered in Microsoft's web browser, Internet Explorer, which could allow an attacker to take complete control of an affected system. Exploitation may occur if a user visits or is redirected to a web page which is specifically crafted to take advantage of these vulnerabilities. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Internet Explorer 6
- Internet Explorer 7
- Internet Explorer 8

RISK: Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:
Seven vulnerabilities have been discovered in Microsoft Internet Explorer. Details of these vulnerabilities are as follows:

HTML Object Memory Corruption Vulnerability
Two remote code execution vulnerabilities exist in the way that Internet Explorer accesses an object that has not been correctly initialized or has been deleted. Exploitation may occur if a user visits a web page that is specifically crafted to take advantage of these vulnerabilities. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Cross-Domain information Disclosure Vulnerability
Two information disclosure vulnerabilities exist in Internet Explorer that could allow a remote attacker access to sensitive data. Exploitation may occur if a user visits a web page that is specifically crafted to take advantage of this vulnerability. Successful exploitation of this vulnerability could result in an attacker gaining access to another domain or Internet Explorer zone.

HTML Element Memory Corruption Vulnerability
Two remote code execution vulnerabilities exist as a result of Internet Explorer not being able to access an object that has been removed or not initialized correctly. Exploitation may occur if a user visits a web page that is specifically crafted to take advantage of these vulnerabilities. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Uninitialized Memory Corruption Vulnerabilities
A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that has not been correctly initialized or has been deleted. Exploitation may occur if a user visits a web page that is specifically crafted to take advantage of these vulnerabilities. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Microsoft is reporting that this vulnerability is being exploited in targeted attacks.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:

Microsoft:
http://www.microsoft.com/technet/security/bulletin/ms10-090.mspx

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3340
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3342
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3343
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3345
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3346
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3348
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3362